UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,979	08/31/2000	Adrian Shields	8490.00	3073

7590 09/07/2004

Michael Chan
Intellectual Property Section
Law Department NCR Corporation
101 West Schantz ECD-2
Dayton, OH 45479-0001

EXAMINER
PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>21 May 2004</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-20</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-20</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>21 May 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

        1.☒ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-36 are pending.

2.   The amendment of 5/21/2004 (paper no. 4) has been received and considered.

Drawings

3.   The corrected or substitute drawings were received on 5/21/2004.   These drawings are acceptable for examination purposes only.   Formal drawings will be required when the application is allowed.

Specification

4.   In view of the amendment made to the paragraphs one pages 6 and 7, the objection to the specification made in the earlier Office action is hereby withdrawn.

Claim Rejections - 35 USC § 112

5.   In view of the amendment made to claim 1, the rejection made in the earlier Office action for a 112 1st is hereby withdrawn.

6.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly
> pointing out and distinctly claiming the subject matter which the applicant
> regards as his invention.

7.   Claim 7 is rejected under 35 U.S.C. 112, second paragraph,

as being indefinite for failing to particularly point out and

distinctly claim the subject matter which applicant regards as

the invention.

8.   Claim 7 recites the limitation "the challenge value" in

line 2. There is insufficient antecedent basis for this

limitation in the claim.

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which

forms the basis for all obviousness rejections set forth in this

Office action:

> (a) A patent may not be obtained though the invention is not identically
> disclosed or described as set forth in section 102 of this title, if the
> differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at
> the time the invention was made to a person having ordinary skill in the
> art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

10. Claims 1, 3, 5, 10, 13-14, 16-17 rejected under 35

U.S.C. 103(a) as being unpatentable over Kawan (U.S.

2002/0062284) and further in view of McNair (U.S. 5,278,905).

As per claim 1, Kawan discloses a display for displaying

financial transaction options, an input for receiving financial

data for a financial transaction (see paragraph 28), and means for encrypting the financial data with a key (see paragraph 31).

Kawan fails to disclose means for generating a new key for the financial transaction, wherein the key is generated using one or more variable properties of the portable terminal.

However McNair discloses means for generating a new key for the financial transaction, wherein the key is generated using one or more variable properties of the portable terminal (see column 4 lines 28-40).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use McNair's method of key generation for the key used in Kawan's encrypting means.

Motivation to do so would have been to protect an attacker from recording an encrypted string and sending that for the attackers own service request (see column 4 lines 19-31).

As per claim 3, the modified Kawan and McNair system discloses the one or more variable properties of the portable terminal include date and time settings (see column 4 lines 28-40).

As per claim 5, the modified Kawan and McNair system discloses a display for displaying financial transaction options, an input for receiving financial data for a financial transaction (see Kawan paragraph 28), means for generating a new

key for the financial transaction, wherein the key is generated

using one or more variable properties of the portable terminal

(see McNair column 4 lines 28-40) and means for encrypting the

financial data with a key (see Kawan paragraph 31).

As per claim 10, the modified Kawan and McNair system

discloses a self-service terminal a portable terminal to execute

an encryption program (see Kawan paragraphs 29 and 31) which is

operable to use one or more variable properties of the portable

terminal for obtaining a sequence of values for generating a new

key based on the sequence of values (see McNair column 4 lines

28-40), and the portable terminal encrypting information for a

financial transaction with the new key, and the portable

terminal wirelessly transmitting encrypted information to the

self service terminal (see Kawan paragraphs 29 and 31).

As per claim 13, the modified Kawan and McNair system

discloses a user interface having display for displaying

financial transaction options, an input for receiving financial

data for a financial transaction (see Kawan paragraph 28),

memory for storing an encryption program, a controller for

executing the encryption program (see Kawan paragraph 31) to

generate a new key for the financial transaction, wherein the

key is generated using one or more variable properties of the

portable terminal (see McNair column 4 lines 28-40), the

controller encrypting information for a financial transaction

with the new key, and a communication port to wirelessly

transmitting encrypted information to the self service terminal

(see Kawan paragraphs 29 and 31).

As per claim 14, the modified Kawan and McNair system

discloses the portable terminal being a PDA and the encrypted

information being transmitted to an ATM (see Kawan paragraph

29).

As per claim 16, the modified Kawan and McNair system

discloses the user interface is a keypad and the financial

transaction data includes a personal identification number (see

Kawan paragraph 31).

As per claim 17, the modified Kawan and McNair system

discloses the personal identification number being biometric

based (see Kawan paragraph 31).

11.   Claim 2 is rejected under 35 U.S.C. 103(a) as being

unpatentable over the modified Kawan and McNair system as

applied to claim 1 above, and further in view of Chaum (U.S.

4,539,870).

The modified Kawan and McNair system fails to disclose the

key being generated when the transaction is executed.

However, Chaum discloses generating a new key when the

transaction is executed (see column 12 lines 3-7).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to generate a key when the transaction is executed as described by Chaum in the modified Kawan and McNair system.

Motivation to do so would have been to for temporary keys (see Chaum column 12 lines 3-7).

12.   Claims 4, 6-9, 11-12, 15, 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over modified Kawan and McNair system as applied to claims 1 and 5 above, and further in view of Menezes et al, Handbook of Applied Cryptography, CRC Press, 1997 (herein after Menezes).

As per claim 4, the modified Kawan and McNair system fails to disclose generating a unique challenge that can be issued for each transaction.

However, Menezes discloses the use of a unique challenge for each transaction (see 10.3, 10.3.1 and 10.9 on page 397).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the unique challenge of Menezes in the modified system of Kawan and McNair.

Motivation to do so would have been to prove the identity between entities (see Menezes 10.3 pg. 397).

As per claim 6, which adds the further limitation of the unique challenge being based on the sequence of values. Menezes

discloses this in section 10.3 on page 397 where the entities

prove the identity by the knowledge of a secret associated with

each entity (the encryption key which is based on the sequence

of values).

As per claim 7, which adds the further limitation of

encrypting the new key and challenge using a public key (see

Menezes section 10.3.3 pages 403-404).

As per claim 8, the modified Kawan, McNair and Menezes

system discloses using one or more properties of the portable

terminal to obtain a sequence of values, generating a new key

based on the sequence of values (see McNair column 4 lines 28-

40), generating a challenge value based on the sequence of

values (see Menezes page 397 as applied in claim 6), encrypting

the new key and challenge using a public key (see Menezes

section 10.3.3 pages 403-404) and transmitting this encrypted

message to the self-service terminal (see Kawan paragraphs 29

and 31).

As per claim 9, the modified Kawan, McNair and Menezes

system discloses generating a new challenge value at the self-

service terminal, encrypting the challenge using the new key,

transmitting it to the portable terminal (see Menezes section

10.3.3 pages 403-404 being performed in the self-service

terminal of Kawan), and awaiting the correct response to the

transmitted challenge value being transmitted by the portable

terminal before accepting any subsequent transaction at the

self-service terminal (this is inherent from the idea of the

challenge used to authenticate an entity before communicating

with that entity as described in Menezes).

As per claim 11, the modified Kawan, McNair, and Menezes

system discloses using one or more properties of the portable

terminal to obtain a sequence of values, generating a new key

based on the sequence of values (see McNair column 4 lines 28-

40), generating a challenge value based on the sequence of

values (see Menezes page 397 as applied in claim 6), encrypting

the new key and challenge using a public key (see Menezes

section 10.3.3 pages 403-404) and transmitting this encrypted

message to the self-service terminal (see Kawan paragraphs 29

and 31) transmitting a response to the message to the portable

terminal (see Menezes section 10.3.3 pages 403-404 being

performed in the self-service terminal of Kawan), and halting

any further transmission unless the decrypted response includes

the correct reply to the challenge value (this is inherent from

the idea of the challenge used to authenticate an entity before

communicating with that entity as described in Menezes).

13.   Claims 12, 18 are rejected under 35 U.S.C. 103(a) as being

unpatentable over the modified Kawan and McNair system as

applied to claims 1, 13 above, and further in view of Menezes.

As per claim 12, the modified Kawan and McNair system fails

to disclose the one or more variable properties includes data

stored in a dynamic heap of a memory.

However, Menezes discloses this on page 172 for the content

of the input/output buffers where a heap is defined as an area

of memory used for dynamic memory allocation and buffer is

defined as an area of memory used for storing messages, and the

input and output are constantly changing making the buffer

dynamic.

At the time of the invention it would have been obvious to

a person of ordinary skill in the art to use Menezes method for

creating a key based on dynamic heap of a memory in the modified

system of Kawan, McNair, and Menezes.

As per claim 18, the modified system of claim 12 discloses

the one or more variable properties includes usage history

stored in the memory (see Menezes page 172 (ii) #2.).

14.   Claims 15 and 19 are rejected under 35 U.S.C. 103(a) as

being unpatentable over the modified Kawan and McNair system as

applied to claim 5, 13 above, and further in view of Menezes.

As per claim 15, the modified Kawan and McNair system fails
to disclose the use of a symmetric key.

However, Menezes discloses the use of a symmetric key (see
section 1.5).

At the time of the invention it would have been obvious to
a person of ordinary skill in the art to use a symmetric key
from Menezes in the modified system of Kawan and McNair.

Motivation to do so would have been the keys for symmetric
keys are relatively short (see Menezes page 31).

As per claim 19, the modified Kawan, McNair and Menezes
system discloses using a public key issued by a host for
encryption (see Menezes section 1.8).

15.   Claim 20 is rejected under 35 U.S.C. 103(a) as being
unpatentable over the modified Kawan, McNair and Menezes system
as applied to claim 8 above, and further in view of Matyas et al
(U.S. 4,941,176).

The modified system of Kawan, McNair and Menezes fails to
disclose splitting a hash value into halves and encrypting the
second half with the first half to produce a key.

However Matyas et al discloses such a method (see column
113 lines 15-44).

At the time of the invention it would have been obvious to
a person of ordinary skill in the art to use Matyas et al's

method for key generation in the modified system of Kawan,

McNair and Menezes.

Motivation to do so would have been to protect against key

half replicating attacks as described in column 113 lines 15-44

of Matyas el at.

Response to Arguments

Applicant's arguments for claims 1-11 are removed based on

amendments and the application of new prior art.

Conclusion

Any inquiry concerning this communication or earlier

communications from the examiner should be directed to Michael

Pyzocha whose telephone number is (571) 272-3875. The examiner

can normally be reached on 7:30am - 5:00pm first Fridays of the

bi-week off.

If attempts to reach the examiner by telephone are

unsuccessful, the examiner's supervisor, Andrew Caldwell can be

reached on (571) 272-3868. The fax phone number for the

organization where this application or proceeding is assigned is

703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

Andrew Caldwell